

How Does Your Email Measure Up?

With the 2016 presidential campaigns under way, Hillary Clinton's use of a personal email account to conduct government business will undoubtedly be in the news for many months to come. Her use of a personal email account raises concerns of public trust, ethics, and security. So far, most of the focus has been on public trust and ethics. This focus is understandable in light of the Freedom of Information Act and the general desire for government transparency. After all who can you trust to willfully hand you their own smoking gun (if one exists)? Amidst the focus on public trust and ethics, the security of the emails has been largely ignored except for the issue of classified information within the emails.

While the Arkansas courts do not deal in classified information, using email to transfer sensitive court information is a serious concern when that information is not properly protected against hackers. There are many aspects to email security that work together to prevent access by these intruders. Email security standards address the physical security of the server, server access, email encryption during storage, encryption of emails across the internet, email system records, data backups, and more. The National Institute of Standards and Technology (NIST) Publication 800-45, Guidelines on Electronic Mail Security, discusses these various standards and is one resource that can be used to judge an email service.

The Arkansas Judiciary is using a broad range of email services throughout the state. These services include free commercial email such as Gmail and Hotmail; locally contracted services such as Comcast and Windstream; internally hosted email through IT departments; and .gov email services administered by the Arkansas Department of Information Systems or Law Enforcement Online (FBI). Currently, the only email requirement for Arkansas Court Automation Program accounts is for users to supply an individual email account. Shared accounts are not acceptable, but .gov email addresses are not currently required. However, use of private email accounts should be avoided. The current email recommendation is for courts to utilize Arkansas Department of Information Systems to obtain .gov email.

Following is a brief explanation of email service types:

? Free Commercial Email Services (Gmail, Hotmail, etc.) (INSECURE)

These email accounts are not secure. While these services often have some security measures in place, user agreements limit or eliminate provider responsibility for that security.

Since any security measures for these services are not assured, they are considered insecure. Additionally, they are problematic in areas of FOIA requests and public trust.

These accounts should be avoided for government business.

? Email services through local paid provider or hosted by court IT department (MAY OR MAY NOT BE SECURE ? ASSUMED INSECURE)

In order to truly assess the security of individual paid providers or local IT departments, a

security determination would have to be made based on the contract with the provider or on the IT department for courts hosting their own email. It is not feasible for the AOC to make this assessment, and the Legislative Audit does not currently assess email based on their Best Practices publication. This option raises concerns of system security, information security, and government accountability and transparency. Courts are generally not equipped to address these concerns.

? .gov email account through DIS (SECURE)

Again, this is the recommended option. These accounts are secure and also provide for government accountability and transparency. The Arkansas Department of Information Systems provides government email accounts for \$9.50 per month per account. If you would like more information, or to obtain accounts, you can contact their help desk at 501-682-4357 or email them at dis.callcenter@arkansas.gov. Their website is located at www.dis.arkansas.gov.

? .gov email account through LEO.gov (SECURE)

This is another way to obtain .gov email accounts that are secure and provide for government accountability and transparency. These Law Enforcement Online accounts are free.

However, guidance from leo.gov support personnel has not been clear, and some court staff have received accounts while others have been denied. You can visit www.leo.gov (resolves to <https://www.cjis.gov/CJISEAI/EAIController>) to apply for an account.

What You Can Do

Although you can protect against insecure email services by using end-to-end encryption, properly setting up the software and exchanging encryption keys can be daunting. Using a secure email service is the best solution for everyday operations. If this is not possible, individual awareness is essential. Know what data is sensitive in your workplace, and avoid sending sensitive data through insecure email services. If you would not want your email contents released to the public, do not send them with insecure email services.

Source URL: <https://courts.arkansas.gov/forms-and-publications/newsletters/friends-court/how-does-your-email-measure>